

How Trust is Propagated in Decentralized Identity Systems

June 2, 2026

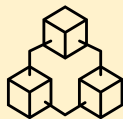
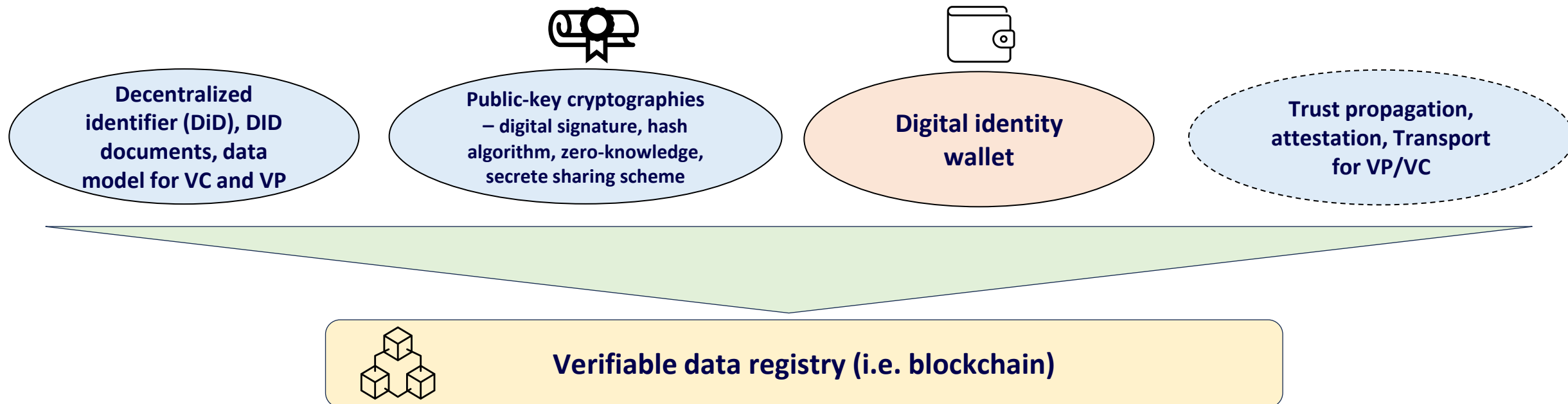
Heung Youl YOUM, PhD

Professor, Soonchunhyang University, Korea (Republic of)
Chairperson, Open Digital Identity Foundation, Korea

Key underlying technologies for decentralized identity system

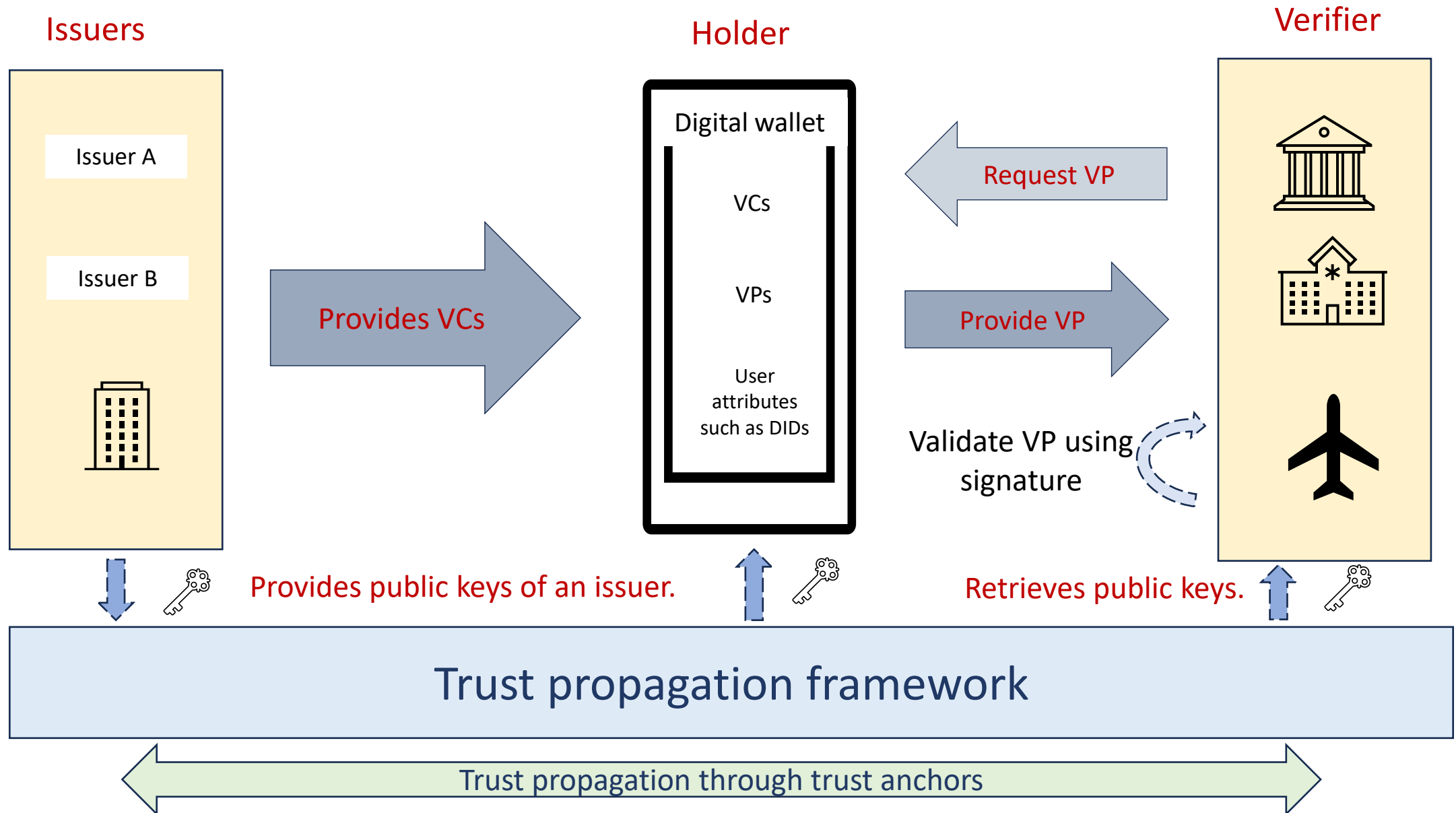
▪ Decentralized identity

- Credential (certificate, ID)
 - A set of one or more claims about a holder made by an issuer. For example, name, age, degree name, etc.
- Verifiable credential
 - A tamper-resistant credential that can be cryptographically verified



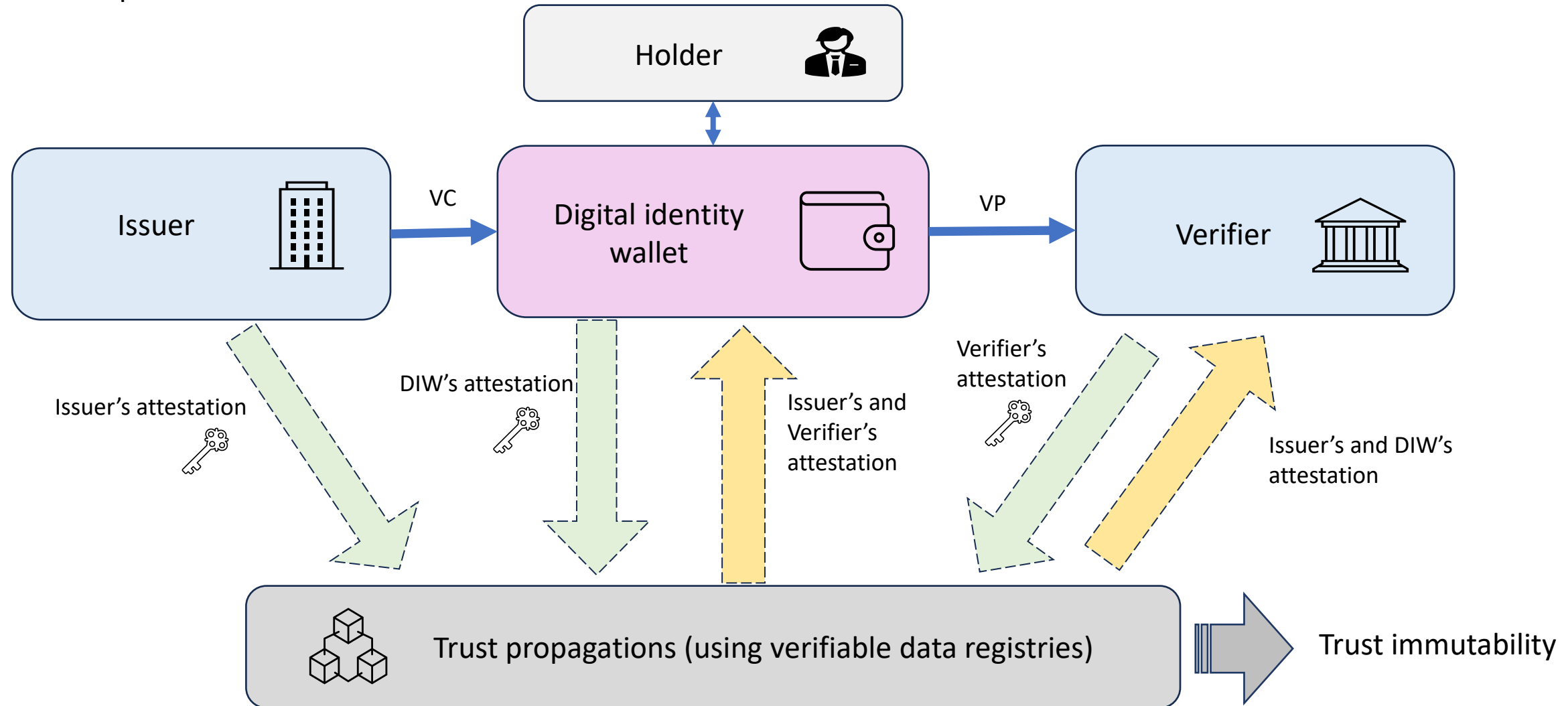
Verifiable data registry (i.e. blockchain)

Digital identity wallet and simple trust propagation for issuers

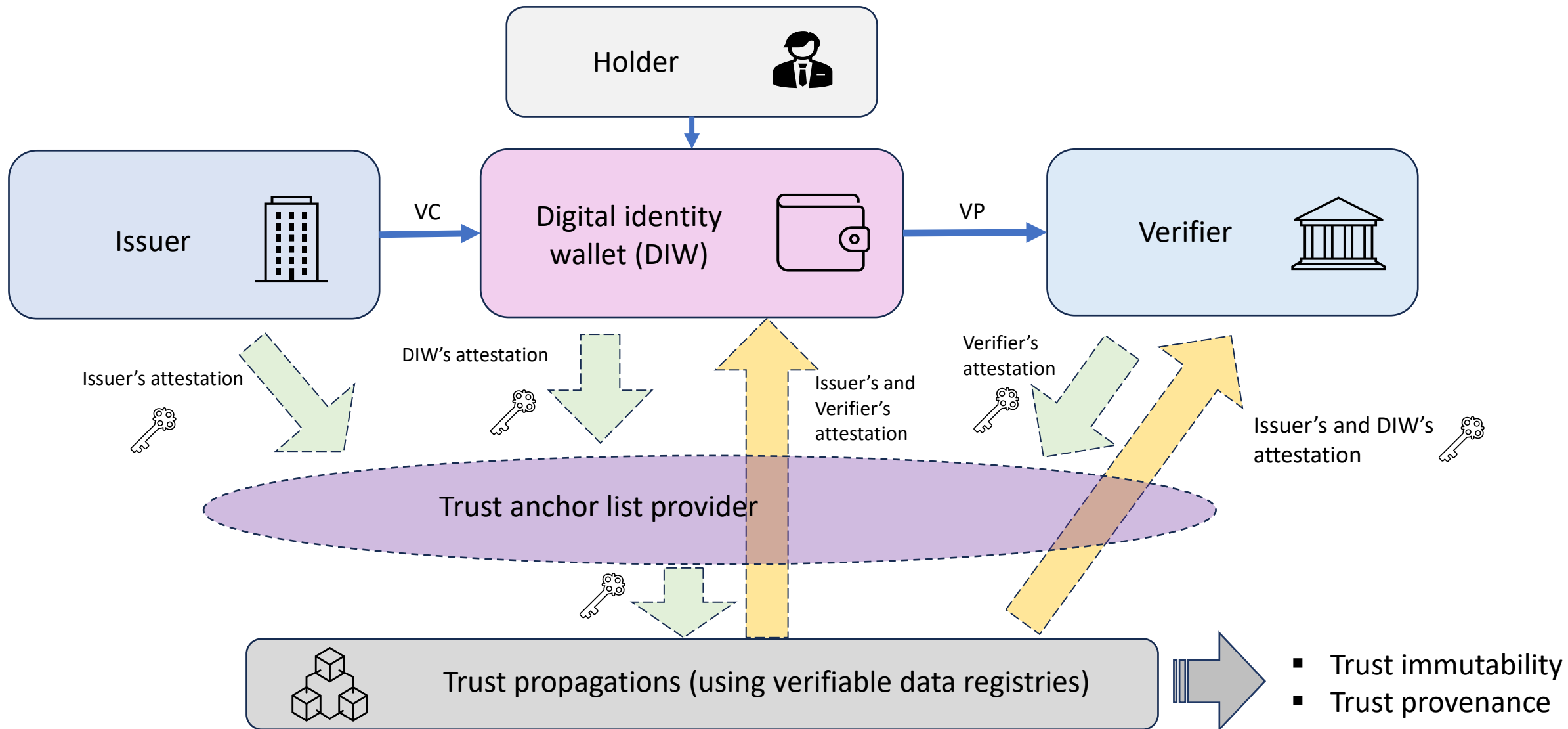


How trust is propagated without trust anchor list provider?

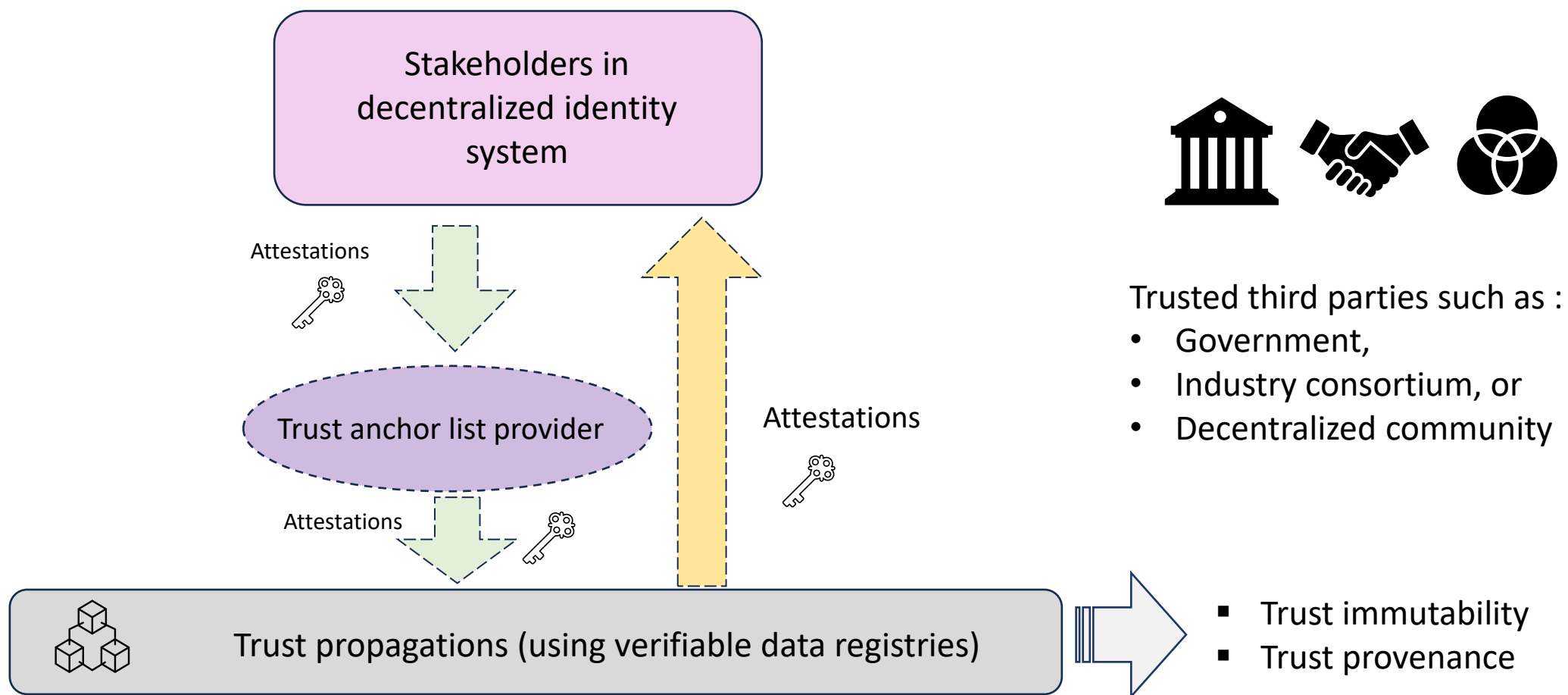
- Trust propagation: process by which trust in an entity gradually spreads across a network based on established relationships and interactions.



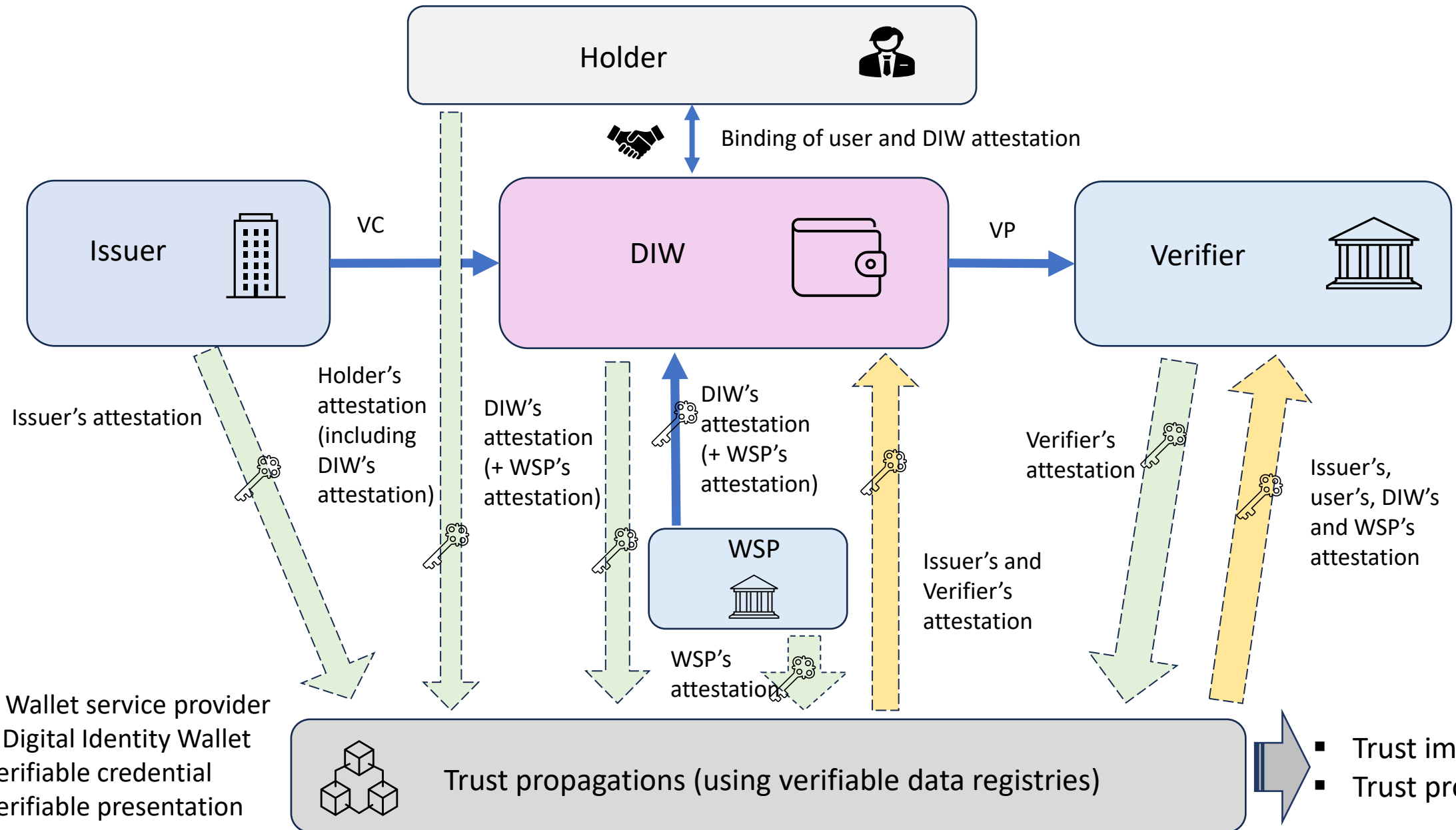
Trust propagation with trust anchor list provider



Who will be a trust anchor list provider?

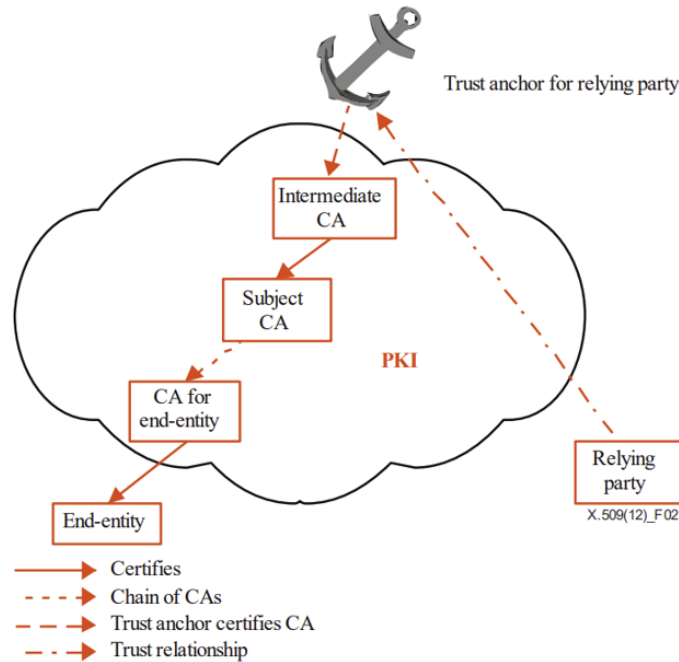


(simplified) Trust framework for mobile ID in Korea

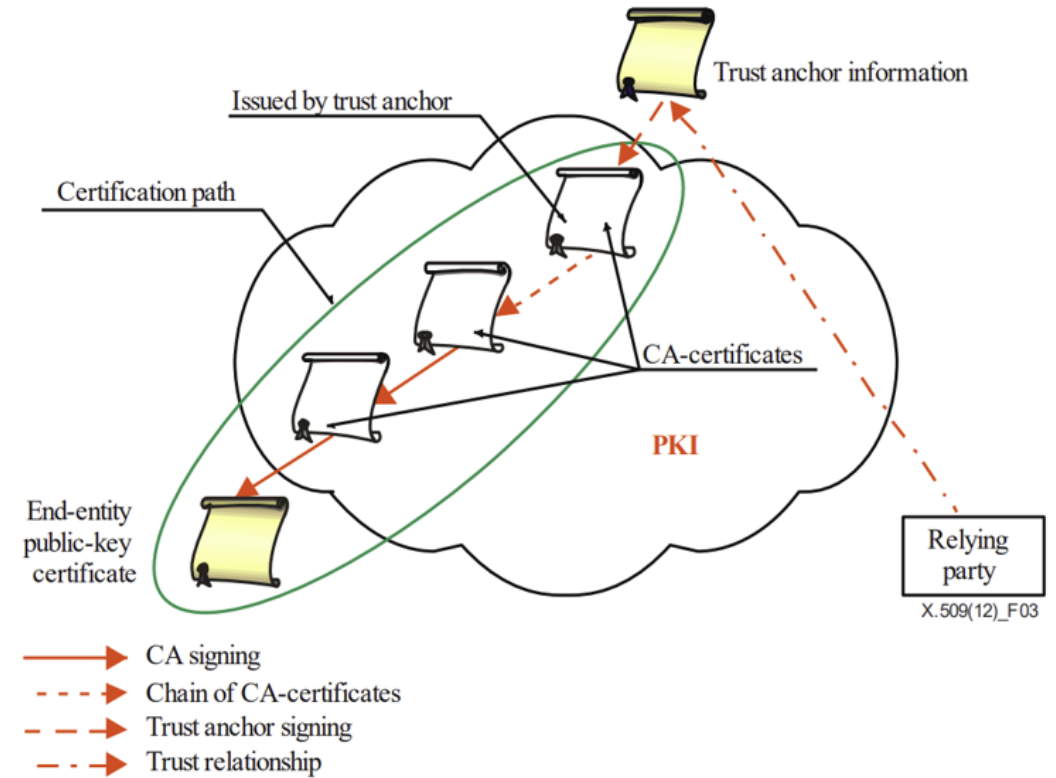


- WSP: Wallet service provider
- DIW: Digital Identity Wallet
- VC: verifiable credential
- VP: verifiable presentation

Concept of PKI-based trust propagation in PKI

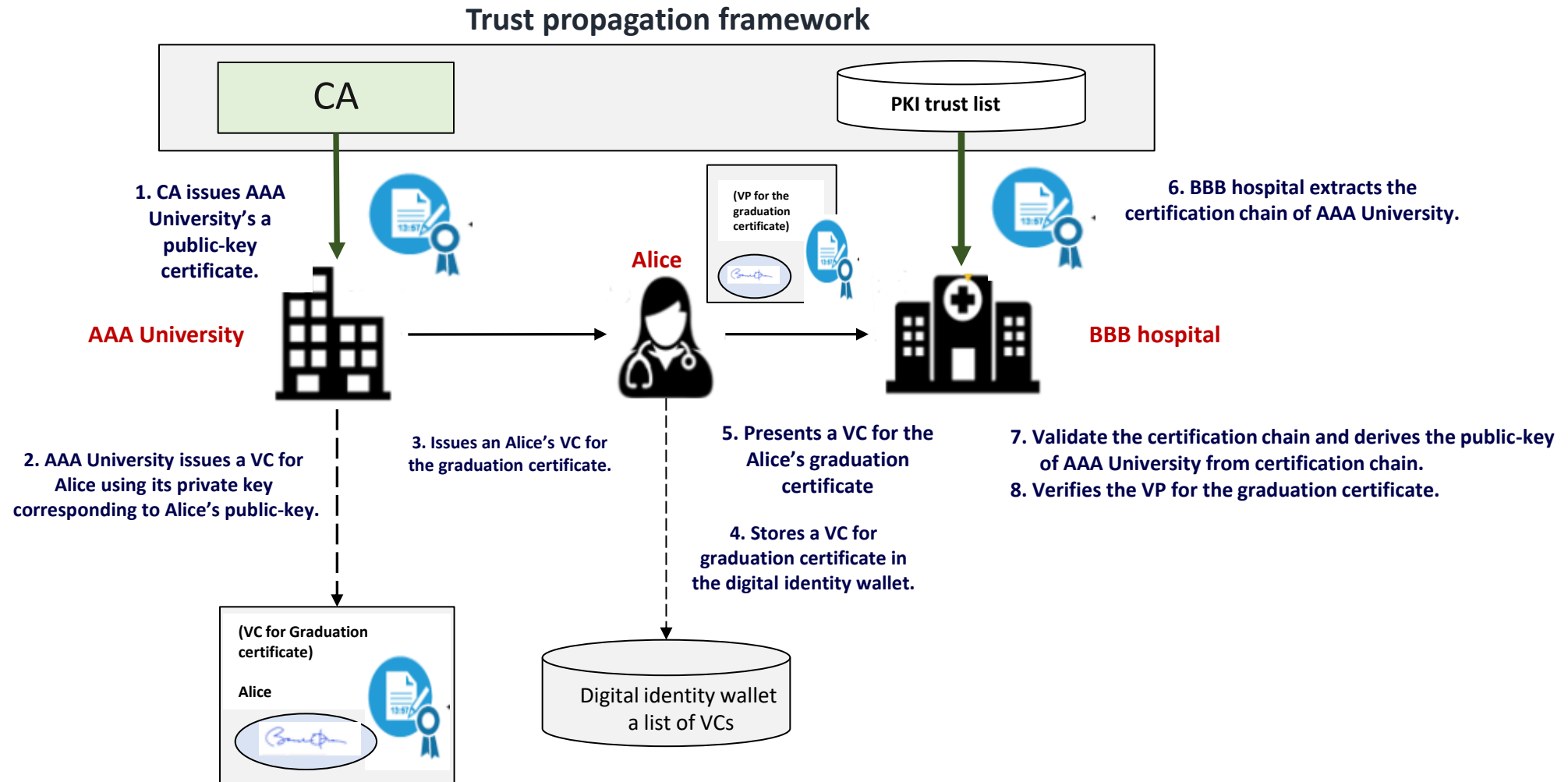


Entity relationships in PKI



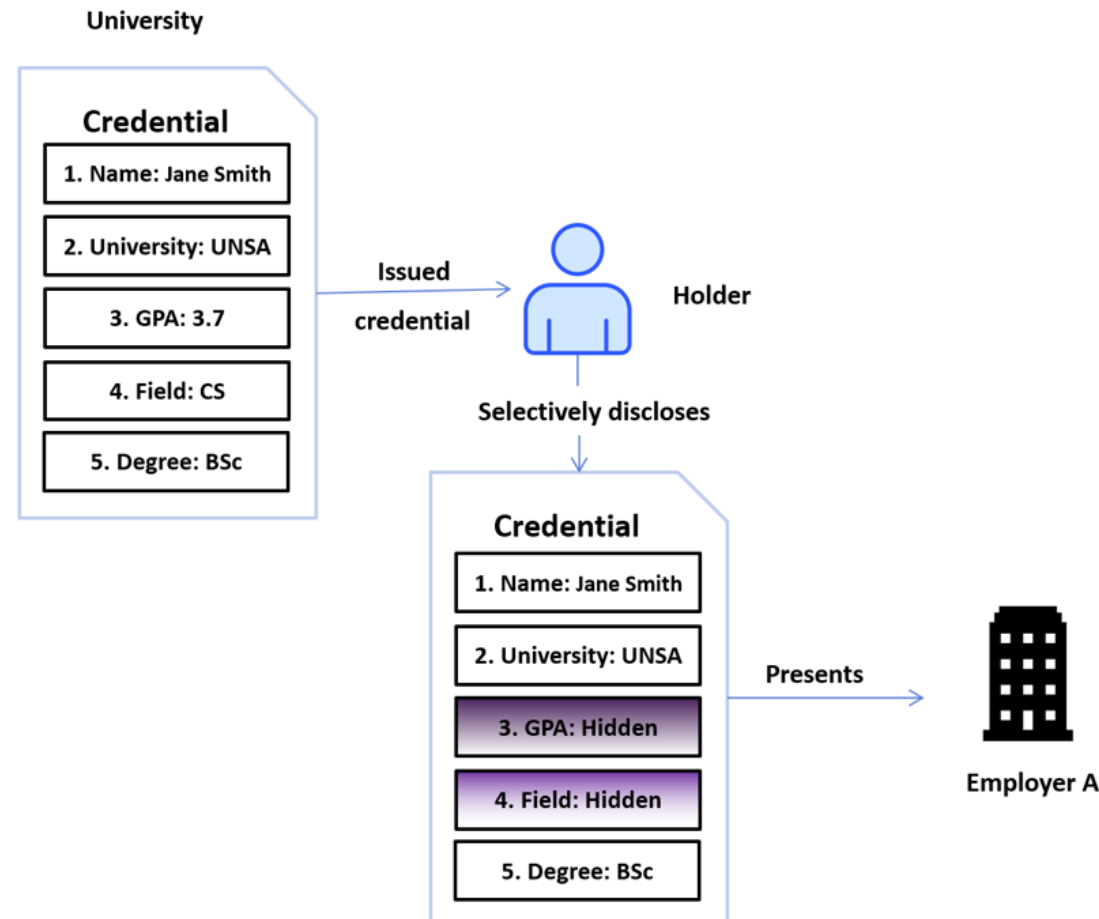
Certification path

PKI-based trust propagation model for decentralized identity

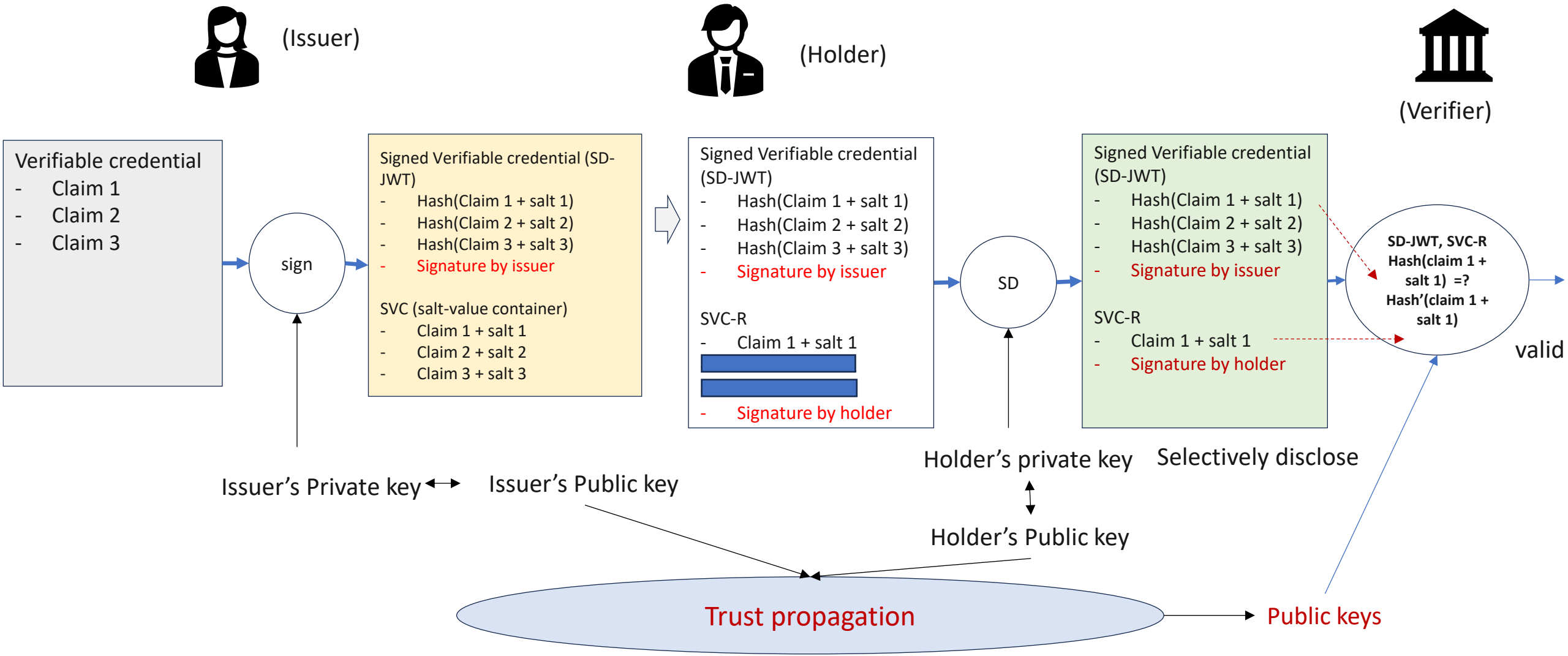


How is privacy ensured in the decentralized identity system?

- **Selective disclosure:** ability of holders to choose specific pieces of information, known as a claim, from their verifiable credentials they want to share with a verifier, allowing them to reveal only the necessary claims while keeping other personal data private.

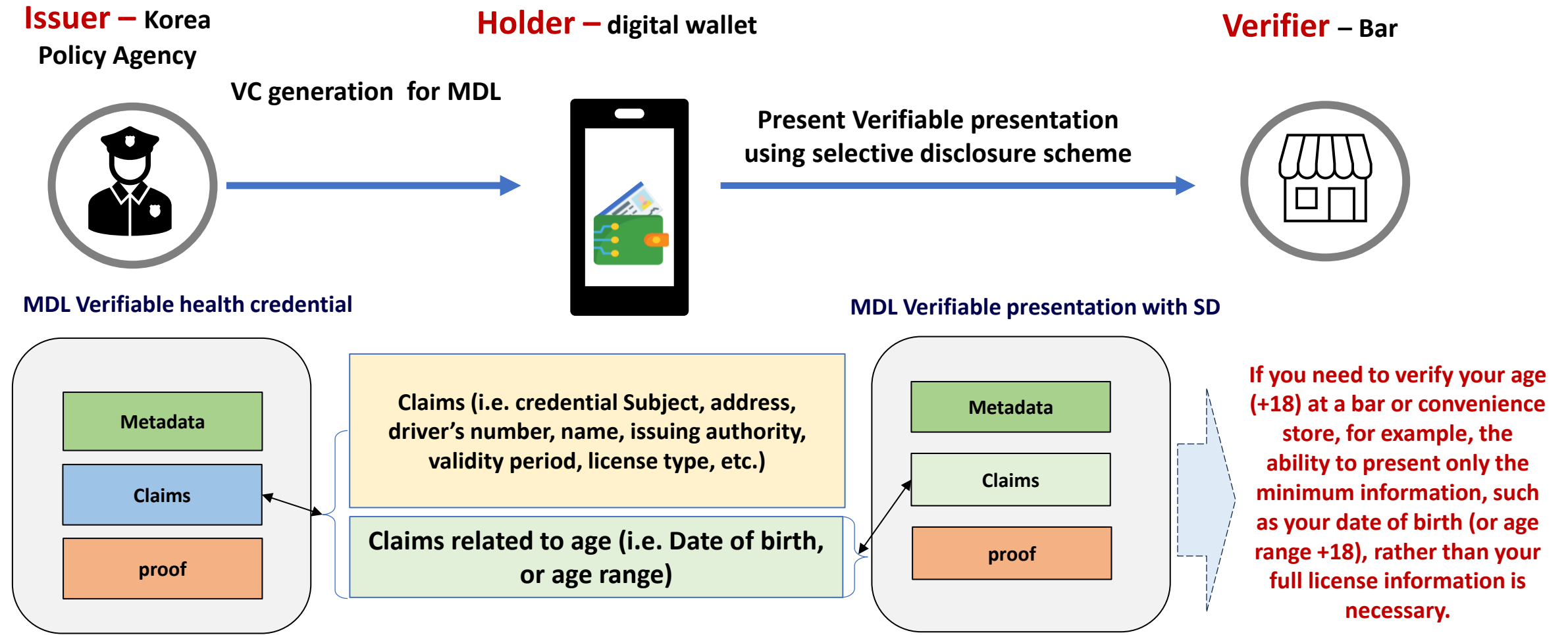


Trust propagation for Selective Disclosure based on hash (SD-JWT)



11

Use case for selective disclosure scheme (age verification) in mobile driver's license in Korea started in 2022

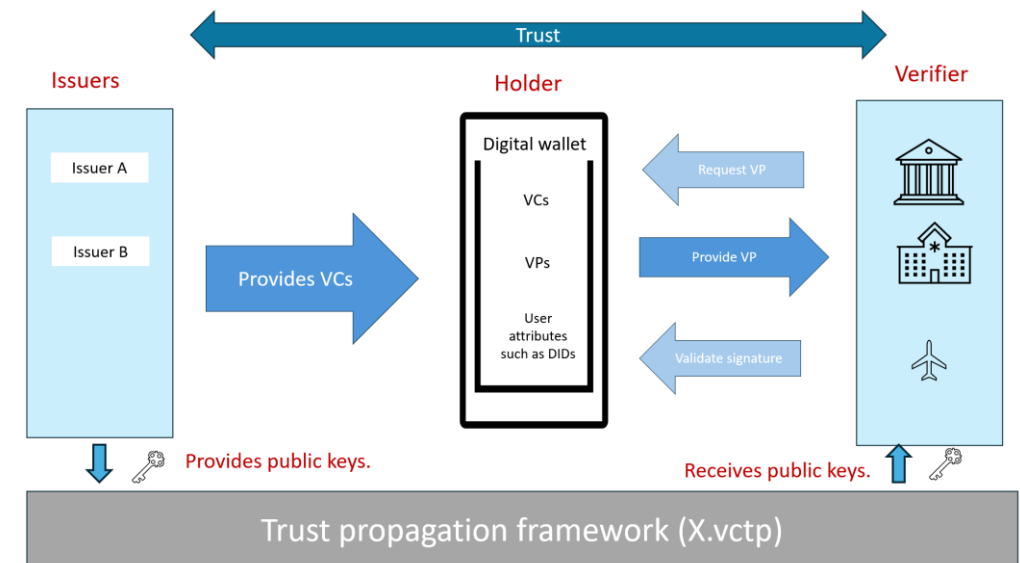


Verifiable credential-based trust propagation framework in the decentralized identity

(ITU-T SG17, ITU-T [X.vctp](#), September 2025)

Trust propagation is a process by which trust in an entity gradually spreads across a network based on established relationships and interactions, allowing entities to assess the trustworthiness of other entities within a decentralized identity system without relying on a central authority. This draft Recommendation provides a verifiable credential-based trust propagation framework in the decentralized identity. It also includes:

- describing two trust propagation models and identifying roles of entities and metadata needed;
- identifying functional components in the DID platform;
- defining metadata for trust propagation;
- describing procedure for this trust propagation;
- describing threats and controls associated with its framework.



Thank you for your
attention

